TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Overview of the HIPAA Security Rule

HIPAA Security • November 2003

Health Insurance Portability and Accountability Act (HIPAA) regulations are divided into four sets of standards or Rules: (1) Privacy, (2) Security (discussed here), (3) Identifiers and (4) Transactions and Code Sets. The Final Security Rule was published in the *Federal Register* in February 2003. DoD must be in compliance with the rule by April 21, 2005.

Unlike the HIPAA Privacy Rule, which applies to protected health information (PHI) in "any form or medium," the Security Rule covers only PHI that is electronically stored or transmitted (EPHI) by covered entities. The Department of Health and Human Services (DHHS) may publish standards to protect health information in other, non-electronic media in a future rule. While the Privacy Rule is focused on protecting the confidentiality of PHI, the Security Rule broadens the focus to include protecting the integrity and availability of the protected information as well.

The objectives of the Security Rule are found in the general requirement. Covered entities that "collect, maintain, use or transmit" EPHI must implement "reasonable and appropriate administrative, physical and technical safeguards" that ensure integrity, availability and confidentiality. Such measures — notably in the form of policies and procedures — must provide protection against "any reasonably anticipated threats or hazards," ensure that the information is used and disclosed only as permitted by the Privacy Rule, and ensure that the covered entity's workforce complies with the security rule.

In comparison to the Privacy Rule, the Security Rule is logically structured and compact. The Security Rule's requirements are divided into administrative, physical and technical safeguards. Each safeguard category is divided into standards and implementation specifications that outline what a covered entity must do to achieve the objectives presented in the general requirement.

The process used in the creation of the administrative, physical and technical safeguards includes three parts:

- "assess potential risks and vulnerabilities" to EPHI;
- "develop, implement and maintain appropriate security measures" given those risks; and
- document those measures and keep them current.

The administrative simplification provisions of HIPAA established three characteristics the security rules needed to conform to. DHHS needed to create standards that were:

- "comprehensive and coordinated," covering all aspects of security;

Overview of the HIPAA Security Rule

- "scalable," and so suitable for covered entities of any size or type; and
- "technology neutral," to allow for changes as security technologies evolve.

The last two of these characteristics enables a flexible approach that allows covered entities to adopt and change protection measures based on their own needs and capabilities as the risk environment and technology changes. Of course this also means that each covered entity must assess its risks and protection strategies on a periodic basis to ensure its safeguards are always "reasonable and appropriate." The rule does not permit a checklist or cookie-cutter approach to compliance. "…entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be usable by all covered entities." (Final Security Rule, p.8335) How a covered entity satisfies individual security requirements and which technologies they use are "business decisions that each entity [has] to make ... reviewing and modifying the measures as needed to continue the provision of reasonable and appropriate protections." (Final Security Rule, pp.8341, 8342)

Note that this Rule establishes only a national "minimum standard" for security of electronic health information. Covered entities may for various reasons need or want to exceed that.

Following is an outline of the Security Rule with links to an explanation of the requirements. If you can not find the answer you are looking for in these entries or elsewhere on this web site, please feel free to contact us.

Security Rule General Requirements

- "electronic" applicability (The who, what, when and where of the Security Rule)
- standards and implementation specifications (required vs. addressable)
- policies and procedures
- documentation

Security standards and implementation specifications

- administrative safeguards
  - security management process
  - assigned security responsibility
  - workforce security
  - information access management
  - security awareness and training
  - security incident procedures
  - contingency plan

TMA Privacy Office Information Paper

Records Management◆FOIA◆DUAs◆HIPAA Compliance◆ADP Security◆Privacy Act◆System of Records◆PIAs

Overview of the HIPAA Security Rule